UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/598,611	09/06/2006	Bogdan Costin Popescu	NL 040288	7824

24737 7590 03/28/2008

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	PAPER NUMBER
2139	
MAIL DATE	DELIVERY MODE
03/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/598,611	POPESCU ET AL.	
	Examiner	Art Unit	
	Christian LaForgia	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 September 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *22-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *22-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 September 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-21 have been cancelled by the Applicant's preliminary amendment of 06 September 2006.

2. Claims 22-35 have been presented for examination.

Priority

3. Acknowledgment is made of applicant's claim for foreign priority.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 22-35 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 22-35 clearly invoke 35 U.S.C. 112, 6th paragraph as noted by their use of "means for" language. In order for such claims to satisfy 35 U.S.C. 112, 2nd paragraph, one of ordinary skill in the art should be "able to identify the structure, material or acts from the description in the specification for performing the recited functions." See MPEP § 2181(III). The specification states at page 17, lines 27-31 that the means can be hardware comprising several distinct elements, a suitably programmed computer, or one and the same item of hardware. Since the specification describes the "means for" in broad generic terms, one of ordinary skill would not be able to identify the structure, material or acts from the description in the specification for performing the recited functions; therefore, the claims fail to adequately satisfy the requirements of 35 U.S.C. 112, 2nd paragraph.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 22 and 27-32 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application Publication No. 2005/0010769 A1 to You et al., hereinafter You.

8. As per claim 22, You teaches a domain manager device for managing a network (paragraphs 0007, 0020, i.e. a server automatically sets information on the device or a manager sets it manually) including a plurality of devices (Figures 1 [blocks 100, 110], 2 [blocks 200, 210], 3 [blocks 300, 310]), comprising:

authentication means for generating a predetermined number of authentication tickets, each respective authentication ticket allowing a device with a first identifier to authenticate itself to a device with a second identifier (Figures 1 [step 120], 2 [step 220], 4, paragraph 0022, i.e. exchanging certificates unique to each device) and for issuing to a new device joining the network a predetermined number of symmetric authentication keys, each respective authentication key allowing authenticated communication with one respective other device in the network (paragraphs 0020-0021, i.e. generating a key using one-way functions for each specific device), the authentication tickets with a first identifier matching an identifier for the new device (Figures 1 [step 120], 2 [step 220], 4 [block 415], paragraph 0022, i.e. exchanging certificates); and

key management means for generating a predetermined number of master device keys, the authentication means being arranged for issuing one of the generated master device keys to the new device, the key management means being arranged for associating each generated master device key with a mutually unique identifier, for assigning to the new device as a device identifier the unique identifier associated with the master device key issued to the new device, and upon the new device ceasing to be part of the network, for generating a new master device key and associating the generated new master device key with the unique identifier assigned previously as the device identifier to the new device (paragraphs 0020-0023).

9. Regarding claims 27 and 28, You teaches wherein the predetermined number of authentication keys is chosen as one less than or as equal to or more than a maximum number of devices that may concurrently be comprised in the network (Figure 4, paragraph 0022, i.e. certificates unique to each device means that there is at least an equal number of authentication keys as the number of devices).

10. Regarding claim 29, You teaches wherein the authentication means is arranged for generating for a particular identifier associated with a particular generated master device key a number of authentication tickets, each generated authentication ticket allowing a device with said particular identifier to authenticate itself to a device with one other of the unique identifiers associated with one of the generated master device keys (paragraphs 0020-0023).

11. As per claim 30, You teaches first device (Figures 1 [block 100], 2 [block 200], 3 [block 300]) arranged to communicate with a second device (Figures 1 [block 110], 2 [block 210], 3 [block 310]) via a network comprising a plurality of devices, the first device comprising:

networking means for requesting to a domain manager device to join the network (paragraphs 0007, 0020, i.e. a server automatically sets information on the device or a manager sets it manually) and for receiving from the domain manager device a predetermined number of symmetric authentication keys, each respective authentication key allowing authenticated communication with one respective other device comprised in the network (paragraphs 0020-0021, i.e. generating a key using one-way functions for each specific device), a master device key (paragraphs 0020-0021, i.e. secret key K = domain ID) and a set of authentication tickets, each respective ticket allowing the first device to authenticate itself to a respective device from the plurality of devices (Figures 1 [step 120], 2 [step 220], 4, paragraph 0022, i.e. exchanging certificates);

authentication means for communicating with the second device using the symmetric authentication key allowing authenticated communication with the second device, the authentication means being arranged to accept the received further authentication ticket as valid if the received further authentication ticket can be successfully decrypted using the master device key, and the authentication means being arranged for distributing to the second device the authentication ticket from the set allowing the first device to authenticate itself to the second device (Figures 4, 5, paragraphs 0022, 0023, i.e. exchanging certificates for mutual authentication in content exchange).

12. Regarding claim 31, You teaches wherein the networking means is arranged for receiving from the second device a further authentication ticket, and the authentication means is arranged to authenticate the second device upon accepting the received further authentication ticket as valid (Figures 1 [step 120], 2 [step 220], 4 [block 415], paragraph 0022, i.e. exchanging certificates).

13. Regarding claim 32, You teaches wherein the authentication means is arranged for deriving a session key from information contained in the distributed ticket and in the received further authentication ticket (Figures 1 [step 130], 2 [step 230], 3 [block 425], paragraphs 0005, 0019, 0022).

Claim Rejections - 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15. Claims 23, 24, 33 and 34 are rejected under 35 U.S.C. 103(a) as being obvious over You in view of U.S. Patent Application Publication No. 2006/0020784 A1 to Jonker et al., hereinafter Jonker.

16. The applied reference appears to have a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art only under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 103(a) might be overcome by: (1) a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was

derived from the inventor of this application and is thus not an invention "by another"; (2) a showing of a date of invention for the claimed subject matter of the application which corresponds to subject matter disclosed but not claimed in the reference, prior to the effective U.S. filing date of the reference under 37 CFR 1.131; or (3) an oath or declaration under 37 CFR 1.130 stating that the application and reference are currently owned by the same party and that the inventor named in the application is the prior inventor under 35 U.S.C. 104, together with a terminal disclaimer in accordance with 37 CFR 1.321(c). This rejection might also be overcome by showing that the reference is disqualified under 35 U.S.C. 103(c) as prior art in a rejection under 35 U.S.C. 103(a). See MPEP § 706.02(l)(1) and § 706.02(l)(2).

17. Regarding claim 23, You does not teach wherein each respective authentication ticket is at least partially encrypted with a master device key from the predetermined number that is associated with the second identifier.

18. Jonker teaches wherein at least part of the certificate is encrypted (paragraph 0164, i.e. encrypted version of key in the right and an AD identifier).

19. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the authentication ticket to be at least partially encrypted and issuing a new one upon failure to decrypt said authentication ticket, since Jonker states at paragraph 0016 that the use of such features in an authentication ticket ensures the secure distribution of content, thereby preventing unauthorized users from accessing and using said content.

20. Regarding claim 24, You does not teach wherein the authentication means is arranged for, upon the key management means detecting that the device identifier assigned to the new

device was previously assigned to another device, issuing a set of replacement authentication tickets to the new device, each respective replacement authentication ticket allowing a device with a first identifier to authenticate itself to the new device and being at least partially encrypted with the master device key associated with the first identifier.

21. Jonker teaches updating a device's rights to access data (paragraphs 0184-0189) and issuing certificates to said devices (paragraph 0154-0157).

22. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the authentication means to be arranged for, upon the key management means detecting that the device identifier assigned to the new device was previously assigned to another device, issuing a set of replacement authentication tickets to the new device, each respective replacement authentication ticket allowing a device with a first identifier to authenticate itself to the new device and being at least partially encrypted with the master device key associated with the first identifier, since Jonker states at paragraph 0016 that the use of such features in an authentication ticket ensures the secure distribution of content, thereby preventing unauthorized users from accessing and using said content.

23. Regarding claim 33, You teaches the authentication means is arranged to distribute to the second device a new authentication ticket allowing the second device to authenticate itself to the first device, the new authentication ticket being at least partially encrypted with the master device key of the second device (Figures 1 [step 120], 2 [step 220], 4, paragraph 0022).

24. You does not teach wherein the authentication ticket is at least partially encrypted and issuing a new one upon failure to decrypt said authentication ticket.

25. Jonker teaches wherein at least part of the certificate is encrypted (paragraph 0164, i.e. encrypted version of key in the right and an AD identifier).

26. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the authentication ticket to be at least partially encrypted and issuing a new one upon failure to decrypt said authentication ticket, since Jonker states at paragraph 0016 that the use of such features in an authentication ticket ensures the secure distribution of content, thereby preventing unauthorized users from accessing and using said content.

27. Regarding claim 34, You does not teach wherein the authentication means is arranged for receiving from the second device a new ticket allowing the first device to authenticate itself to the second device, the new ticket being at least partially encrypted with the master device key of the first device, and for decrypting the new ticket with the master device key and for replacing the ticket from the set allowing the first device to authenticate itself to the second device by the new ticket upon successful decryption of the new ticket.

28. Jonker teaches updating a device's rights to access data (paragraphs 0184-0189) and issuing certificates to said devices (paragraph 0154-0157).

29. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the authentication means to be arranged for receiving from the second device a new ticket allowing the first device to authenticate itself to the second device, the new ticket being at least partially encrypted with the master device key of the first device, and for decrypting the new ticket with the master device key and for replacing the ticket from the set allowing the first device to authenticate itself to the second device by the new ticket upon

successful decryption of the new ticket, since Jonker states at paragraph 0016 that the use of such features in an authentication ticket ensures the secure distribution of content, thereby preventing unauthorized users from accessing and using said content.

30. Claims 25, 26 and 35 are rejected under 35 U.S.C. 103(a) as being obvious over You in view of U.S. Patent Application Publication No. 2005/0220304 A1 to Lenoir et al., hereinafter Lenoir.

31. The applied reference appears to have a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art only under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 103(a) might be overcome by: (1) a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not an invention "by another"; (2) a showing of a date of invention for the claimed subject matter of the application which corresponds to subject matter disclosed but not claimed in the reference, prior to the effective U.S. filing date of the reference under 37 CFR 1.131; or (3) an oath or declaration under 37 CFR 1.130 stating that the application and reference are currently owned by the same party and that the inventor named in the application is the prior inventor under 35 U.S.C. 104, together with a terminal disclaimer in accordance with 37 CFR 1.321(c). This rejection might also be overcome by showing that the reference is disqualified under 35 U.S.C. 103(c) as prior art in a rejection under 35 U.S.C. 103(a). See MPEP § 706.02(l)(1) and § 706.02(l)(2).

32. Regarding claims 25 and 35, You does not teach wherein the networking means is arranged for receiving a local revocation list identifying revoked devices that are comprised in

the network and a number of revocation authentication codes, each respective revocation authentication code enabling authentication of the local revocation list using a respective master device key, the authentication means being arranged for accepting the local revocation list as valid if one of the received revocation authentication codes can be successfully decrypted using the master device key.

33. Lenoir teaches the use of a black list which is a list of device IDs that have been revoked (paragraph 0008).

34. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the networking means to be arranged for receiving a local revocation list identifying revoked devices that are comprised in the network and a number of revocation authentication codes, each respective revocation authentication code enabling authentication of the local revocation list using a respective master device key, the authentication means being arranged for accepting the local revocation list as valid if one of the received revocation authentication codes can be successfully decrypted using the master device key, since Lenoir states at paragraph 0008 that in systems using black lists, all device are trusted by default and that trust can only be revoked, thereby having a low starting overhead.

35. With respect to claim 26, Lenoir teaches wherein the key management means is arranged for generating each respective revocation authentication code by computing a respective keyed message authentication code of the local revocation list using each respective master device key (paragraphs 0044-0062).

Conclusion

36. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

37. The following patents are cited to further show the state of the art with respect to exchange content between domains, such as:

United States Patent No. 6,643,774 B1 to McGarvey, which is cited to show user-delegated tickets used for authentication purposes.

United States Patent Application Publication No. 2006/0212400 A1 to Kamperman et al., which is cited to show a related application with at least one common inventor.

United States Patent Application Publication No. 2003/0084291 A1 to Yamamoto et al., which is cited to show device authentication.

United States Patent Application Publication No. 2003/0076955 A1 to Alve et al, which is cited to show controlling content between devices and domains.

United States Patent Application Publication No. 2005/0081044 A1 to Giles et al., which is cited to show pervasive authentication domains.

38. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

39. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine L. Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

40. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2139

clf